Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 29.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (4 of 5):

- https://estply.com/
- https://estply.com/en/privacy-policy/
- https://estply.com/privaatsuspoliitika/
- https://estply.com/kupsiste-poliitika/

Summary of results

Overall Score: 77 / 100
Status: **Needs Improvement**

Site overall 77 is the mean of 4 pages. Scores range 66 (https://estply.com/) → 84 (https://estply.com/privaatsuspoliitika/). Weakest page: PSI mobile 75 / desktop 73 with mobile LCP 4.8 s (desktop 2.7 s) and Speed Index 7.31 s — the LCP and image-delivery failures are the dominant drag on the score. Page weight is 2.76 MB, of which 2.70 MB is just 8 images, and PSI's image-delivery-insight models 276 KiB of savings. Accessibility is otherwise solid (axe 0 violations, 40 passes, 0 images missing alt), but PSI flags `button-name` and `target-size` both at score 0, and 9 contrast nodes are undetermined. SEO 92 with a missing meta description, and Security basics PASSes while the CSP only sets `frame-ancestors 'self'`, HSTS lacks preload, and Referrer-Policy / Permissions-Policy / COOP / CORP are absent. W3C reports 12 errors, mostly WP Rocket lazyload script markup and malformed srcset/sizes. Desktop is not better than mobile here (73 vs 75, TBT 180 ms desktop vs 0 ms mobile), so the score is not a mobile-only artifact.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
66	75	91	81	92	PASS

 Needs Improvement · https://estply.com/en/privacy-policy/

Score	Performance	Accessibility	Best Practices	SEO	Security
78	90	91	100	85	PASS

 Needs Improvement · https://estply.com/privaatsuspoliitika/

Score	Performance	Accessibility	Best Practices	SEO	Security
84	91	91	100	92	PASS

 Needs Improvement · https://estply.com/kupsiste-poliitika/

Score	Performance	Accessibility	Best Practices	SEO	Security
79	91	91	100	92	PASS

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/	75 / **73**	**4.80 s** / 2.72 s	0.000 / 0.000
https://estply.com/en/privacy-policy/	**90** / 93	**2.55 s** / 722 ms	**0.004** / 0.000
https://estply.com/privaatsuspoliitika/	**91** / 100	**3.45 s** / 721 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika/	**91** / 100	**3.45 s** / 761 ms	0.000 / 0.000

Optimization Checklist

3 of 4 passing — 3 pass · 0 warn · 1 fail · 4 n/a

Item	Status	Detail
Page caching plugin / CDN	**Pass**	Caching plugin detected (WP Rocket)

Item	Status	Detail
active		
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with gzip.
Images lazy-loaded	N/A	No raster elements found (2 SVGs excluded).
Hero image eagerly loaded	**Fail**	Hero image has loading="lazy", which delays LCP (inferred from DOM order/size — Lighthouse LCP element unavailable). Use loading="eager" (or omit loading) and add fetchpriority="high".
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	N/A	Only 2 raster images on the page — responsive-image rule does not apply.
Reasonable number of image sizes	N/A	Too few raster images to evaluate srcset width variety.
JS scripts not blocking in	**Pass**	No render-blocking scripts in .

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Cut mobile LCP (4.8 s) and Speed Index (7.31 s) `Performance`

- **Impact:** LCP, Speed Index, FCP, TTI
- **Problem:** Mobile LCP is 4.8 s vs 2.7 s on desktop and Speed Index is 7.31 s vs 3.15 s; `lcp-breakdown-insight` and `network-dependency-tree-insight` both score 0.
- **Solution:**

- Preload the hero image and keep `fetchpriority="high"` on it:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/10/kaasik-kaupo-kalda-360x640.webp"
imagesrcset="…" imagesizes="…" fetchpriority="high">
```

- Inline the critical CSS for the above-the-fold block and load the 2 external stylesheets non-blocking.
- Flatten the critical request chain shown by `network-dependency-tree-insight` (the document itself took 4.06 s in the runtime capture).
- Re-measure on throttled mobile after the image work below — LCP is image-bound, so fix #2 first.

1B. Shrink the 2.70 MB image payload `Performance`

- **Impact:** LCP, Speed Index, total page weight
- **Problem:** Browser runtime shows 8 images totalling 2.70 MB out of a 2.76 MB page, and PSI's image-delivery-insight estimates 276 KiB of savings.
- **Solution:**
  - Convert the remaining JPEG/PNG assets (e.g. `dsc_5118-324x216.jpg`, `estply-cta-1-520x140.jpg`, the two 251×134 PNGs) to WebP/AVIF; the hero is already WebP.
  - Trim the srcset: 27 distinct widths are generated but only a handful are ever selected — cap at 4–5 breakpoints per image.
  - Serve the 100×100 and 324×216 thumbnails at their real display size rather than upscaled sources.

1C. Name icon buttons and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 (name, role, value), 2.5.8 (target size); PSI accessibility 91
- **Problem:** PSI accessibility is 91 on mobile with `button-name` (weight 10) and `target-size` (weight 7) both scoring 0, even though axe-core reported 0 violations.
- **Solution:**
  - Give every icon-only button an accessible name:

```
<button type="button" aria-label="Open menu"><svg aria-
hidden="true">…</svg></button>
```

  - Ensure interactive targets are at least 44×44 px with adequate spacing (WCAG 2.5.8).

- Re-run axe with the same DOM state PSI used — the two engines disagreeing suggests the buttons are injected after axe's scan.

1D. Load the hero image eagerly with high fetchpriority `Performance`

- **Impact:** LCP, Speed Index
- **Problem:** The optimized-web checklist fails "Hero image eagerly loaded": the first image (`uploads/2026/08/6c041c12…png`) has `loading="lazy"` and no `fetchpriority`, delaying LCP (2.6 s mobile).
- **Solution:** Remove lazy loading from the hero and hint priority:

```
<img src="/wp-content/uploads/2026/08/6c041c12….png"
     alt="…" width="251" height="134"
     loading="eager" fetchpriority="high" decoding="async">
```

  Keep `loading="lazy"` on everything below the fold.

1E. Give every button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 Name, Role, Value; Lighthouse accessibility score
- **Problem:** Lighthouse `button-name` scores 0.00 with weight 10 — "Buttons do not have an accessible name" — even though axe-core reports 0 violations.
- **Solution:**
  - Add visible text or `aria-label` to each `<button>` :

```
<button type="button" aria-label="Close cookie banner">…</button>
```

  - For icon-only buttons, keep the SVG `aria-hidden="true"` and put the label on the button itself.
  - Re-run Lighthouse after the fix to confirm the audit passes.

1F. Enlarge touch targets to at least 24×24 px (44×44 recommended) `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; mobile usability
- **Problem:** Lighthouse `target-size` scores 0.00 with weight 7 — "Touch targets do not have sufficient size or spacing."
- **Solution:**
  - Ensure every link/button hit area is ≥24×24 CSS px with ≥24 px spacing, ideally 44×44.
  - Add padding rather than enlarging the icon:

```
.icon-link { display:inline-flex; align-items:center; justify-content:center; min-width:44px; min-height:44px; }
```

- Check the header nav and footer link lists first — they are the densest clusters on this page.

1G. Cut mobile LCP from 3.5 s by removing render-blocking CSS `Performance`

- **Impact:** LCP, Speed Index, FCP
- **Problem:** Mobile LCP is 3.5 s versus 0.7 s on desktop; Lighthouse flags render-blocking-insight with est. 710 ms savings and unused-css-rules at 32 KiB, plus forced-reflow-insight.
- **Solution:**
  - Enable WP Rocket's **Remove Unused CSS** (or Optimize CSS delivery) so the 2 external + 3 inline stylesheets (9.6 KB) stop blocking first paint.
  - Inline the above-the-fold critical CSS and load the rest with `media="print" onload="this.media='all'"`.
  - Batch DOM reads/writes to eliminate the forced reflow Lighthouse reports.
  - Verify the real LCP element in DevTools Performance panel — the checklist's "hero image lazy-loaded" flag points at a 251×134 PNG, which is almost certainly not the LCP element on this page.

1H. Give the mobile menu toggle an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2, screen-reader and keyboard navigation
- **Problem:** axe reports 1 critical violation — `button-name` on `.header__toggle` — and PSI's `button-name` audit scores 0.00 with weight 10.
- **Solution:** Add visible or programmatic text to the toggle:

```
<button class="header__toggle" aria-label="Ava menüü" aria-expanded="false" aria-controls="main-nav">
  <span class="visually-hidden">Ava menüü</span>
</button>
```

If an icon font/SVG is used, keep `aria-hidden="true"` on the icon so the label is the only accessible name.

1I. Stop 429 rate-limiting of static CSS, JS and font assets `Performance`

- **Impact:** Rendering, LCP, FCP, first-paint stability
- **Problem:** The runtime capture logged 15 console events: `global.3578d4f092e5450b.css` and `core.f7cdefef576df16e.css` were refused because the 429 response was served as `text/html`,

`core.7c21cc2eb9f1534d.js` and `wpr-beacon.min.js` were refused for the same reason, and all three Open Sans `.woff2` files returned 429.

- **Solution:**
  - Identify the rate limiter (WP Rocket, ZoneOS/WAF, or a security plugin) and exclude `/wp-content/` static assets from request throttling.
  - Ensure 429 responses never replace a stylesheet/script with an HTML error body — serve a proper status with the correct `Content-Type`, or better, don't throttle static files at all.
  - Verify by loading the page with a cold cache and confirming zero `net::ERR_ABORTED` / 429 entries in DevTools.
  - If the 429s were triggered by the audit's parallel request burst, re-run the capture to confirm the page renders styled for real users.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Add a meta description `SEO`

- **Impact:** SERP snippet, SEO score (92)
- **Problem:** HTML inventory reports `Description: not set` and PSI fails the `meta-description` audit.
- **Solution:** Add a 150–160 character description per language, since the site has `hreflang` for `et` and `en`:

```
<meta name="description" content="ESTPLY toodab kvaliteetset
kasevineeri Jõgevamaa kaasaegses vineeritehases – usaldusväärne
valmistoode Sinu ärile.">
```

2B. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is only `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, and no script/resource restrictions; Security basics marks "CSP is strict" as fail.
- **Solution:** Deploy a nonce-based policy rather than a flat allowlist:

```
Content-Security-Policy: default-src 'self'; script-src 'nonce-
{random}' 'strict-dynamic' https:; object-src 'none'; base-uri
'none'; frame-ancestors 'self'; upgrade-insecure-requests
```

Note the site has no auth, payments or checkout, so this is defense-in-depth rather than a live exposure — but the header already exists, so making it meaningful is

cheap.

2C. Fix the 12 W3C validation errors `Best Practices`

- **Impact:** Markup validity, lazy-loading correctness, srcset selection
- **Problem:** The validator reports 12 errors: 5× `type="text/rocketlazyloadscript"` combined with `defer`, an empty `href` on a `dns-prefetch` link, `src` on a `<source>` element, `sizes="auto"` without `loading="lazy"`, and two `srcset` values missing width descriptors.
- **Solution:**
  - Configure WP Rocket to emit valid lazyload markup, or drop the `defer` / `async` attributes on the `text/rocketlazyloadscript` data blocks.
  - Remove the empty prefetch link: `<link data-rocket-prefetch href="" rel="dns-prefetch">`.
  - Use `srcset` on `<source>`, not `src`.
  - Add `loading="lazy"` to the image using `sizes="auto"`, and give every `srcset` candidate a width descriptor:

```
<img src="…-251x134.png" srcset="…-251x134.png 251w, …-502x268.png
502w" sizes="(max-width: 600px) 100vw, 251px" loading="lazy"
width="251" height="134" alt="">
```

2D. Add Referrer-Policy, Permissions-Policy, COOP/CORP and SRI `Security`

- **Impact:** Information leakage, cross-origin isolation, third-party script integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, and the single cross-origin script (`cdn.jsdelivr.net/.../iframemanager.js`) has no `integrity` attribute.
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

And pin the CDN script:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist
/iframemanager.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

2E. Cut render-blocking resources to fix the 7.0 s Speed Index `Performance`

- **Impact:** Speed Index, FCP, LCP
- **Problem:** Speed Index is 7.04 s on mobile (2.64 s desktop) and the render-blocking insight estimates 730 ms of savings; 2 external stylesheets plus 3 inline blocks (9.6 KB) are in the critical path.
- **Solution:**
  - Inline the critical above-the-fold CSS and defer the rest (`media="print" onload="this.media='all'"`).
  - Preload the two external stylesheets with `<link rel="preload" as="style">` .
  - Audit the 3 inline style blocks (9.6 KB) — move non-critical rules into the deferred bundle.
  - Re-check the network dependency tree insight after the change; it currently scores 0.00.

2F. Fix invalid script type + defer/async combinations `Best Practices`

- **Impact:** W3C validity, HTML conformance
- **Problem:** W3C reports 8 errors, 6 of them from `<script type="text/rocketlazyloadscript">` carrying `defer` (×5) or `async` (×1) — a data-block type must not use those attributes.
- **Solution:** WP Rocket rewrites script types for lazy execution. Either:
  - Configure WP Rocket's "Delay JavaScript execution" to emit valid markup, or
  - Exclude the affected scripts (cookieyes, Google tag) from delay so they keep `type="text/javascript"` .
  - Also drop the redundant `type="text/javascript"` flagged in 2 warnings.

2G. Harden the WordPress install path `Security`

- **Impact:** Brute-force / takeover surface
- **Problem:** Security basics warns that `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**

```
<Files "install.php">
  Require all denied
</Files>
```

  - Move the login to a custom path (e.g. a security plugin's custom login URL) and add rate limiting / 2FA.

- Keep xmlrpc.php blocked (already passing).

2H. Replace vague "here" link text `SEO`

- **Impact:** WCAG 2.4.4, Lighthouse `link-text`
- **Problem:** The `link-text` SEO audit fails with 2 links lacking descriptive text, and the inventory flags "here" ×2 plus repeated "about us", "products", "contact" etc.
- **Solution:**
  - Rewrite anchor text to describe the destination: "read our cookie policy" instead of "here".
  - Where the visible text must stay short, add `aria-label` with the full purpose.

2I. Enlarge touch targets to 44×44 px `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; mobile usability
- **Problem:** Lighthouse `target-size` scores 0.00 at weight 7 — "Touch targets do not have sufficient size or spacing" — and the SEO `tapTargets` audit also fails.
- **Solution:**
  - Ensure every link/button is at least 44×44 CSS px with ≥8 px spacing.
  - Pay particular attention to footer and cookie-banner controls, which are typically the smallest.

```
a, button { min-width: 44px; min-height: 44px; }
```

2J. Block /wp-admin/install.php and restrict /wp-login.php `Security`

- **Impact:** WordPress attack surface
- **Problem:** Security basics flags the installer at `/wp-admin/install.php` as reachable and the login form served on the default `/wp-login.php` path.
- **Solution:**

```
# Block the installer entirely
<Files "install.php">
  Require all denied
</Files>

# Restrict login to known IPs, or rename via a plugin
<Files "wp-login.php">
  Require ip 203.0.113.0/24
</Files>
```

  - Add rate limiting / 2FA on the login endpoint.

2K. Fix srcset entries missing width descriptors `Best Practices`

- **Impact:** Responsive image selection; W3C validity
- **Problem:** W3C reports 2 errors: `srcset` on the two `<img>` elements has no width specified while `sizes` is present, so browsers cannot pick a candidate.
- **Solution:** Add a width descriptor to each candidate:

```
<img src="…6c041c12….png"
     srcset="…6c041c12….png 251w"
     sizes="251px"
     width="251" height="134" alt="" loading="lazy">
```

  - Or drop `srcset` / `sizes` entirely for these two fixed-size decorative images.

2L. Reduce mobile LCP from 3.5 s `Performance`

- **Impact:** LCP, Speed Index, FCP
- **Problem:** Mobile LCP is 3.5 s (desktop 0.8 s); PSI flags render-blocking resources (est. 280 ms savings), 32 KiB of unused CSS, and 20 KiB of image-delivery savings.
- **Solution:**
  - Inline critical above-the-fold CSS and defer the two external stylesheets.
  - Remove unused CSS rules (32 KiB) — purge unused selectors from the theme's `global` / `core` bundles.
  - Preload the LCP element's image/font and serve it in WebP/AVIF.
  - Re-check with `render-blocking-insight` and `unused-css-rules` in PSI after the change.

2M. Fix invalid `defer` / `async` on WP Rocket lazyload script blocks `Best Practices`

- **Impact:** HTML validity, script execution order
- **Problem:** W3C reports 8 errors, including 5× `defer` and 1× `async` on `<script type="text/rocketlazyloadscript">` data blocks (first at line 23).
- **Solution:** WP Rocket's `text/rocketlazyloadscript` type is a data block, so `defer` / `async` are invalid there. Either:
  - Let WP Rocket rewrite the tag to a real `type="text/javascript"` with `defer` at execution time, or
  - Remove `defer` / `async` from the data-block markup and keep the attributes in the plugin's own config. Also drop the redundant `type="text/javascript"` on line 356 (W3C warning).

2N. Add width descriptors to `srcset` candidates `Best Practices`

- **Impact:** HTML validity, responsive image selection
- **Problem:** W3C reports 2 errors: `srcset` on the two upload PNGs has no width specified while `sizes` is present (lines 482 and 502).
- **Solution:**

```
<img src="…6c041c12….png"
     srcset="…6c041c12….png 800w, …6c041c12-400.png 400w"
     sizes="(max-width: 800px) 100vw, 800px"
     width="800" height="450" alt="" loading="lazy">
```

  Every candidate in a `srcset` must carry a `w` descriptor when `sizes` is used.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. HSTS preload, block install.php, trim the Server header `Security`

- **Impact:** Transport hardening, takeover surface, fingerprinting
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`; `/wp-admin/install.php` is reachable; and the `Server: Apache / ZoneOS` header discloses the stack.
- **Solution:**
  - Append `; preload` to HSTS and submit the domain at hstspreload.org.
  - Block the installer in `.htaccess`:

```
<Files "install.php">
  Require all denied
</Files>
```

  - Suppress the version banner: `ServerTokens Prod` and `Header unset Server`.

3B. Manually verify the 9 undetermined contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe-core returned 9 `color-contrast` nodes it could not resolve (alpha transparency or gradient backgrounds), so contrast is unverified rather than passing.
- **Solution:**
  - Inspect each node in DevTools with the contrast checker against its actual composited background.

    - Target ≥4.5:1 for body text and ≥3:1 for large text; flatten semi-transparent overlays where possible.

3C. Give the JSON-LD a real type and disambiguate repeated link text `SEO`

- **Impact:** Rich results eligibility, anchor-text clarity
- **Problem:** The single JSON-LD block parses but its type is reported as `Unknown`, and 8 link texts repeat (e.g. "kontakt" ×2, "meist" ×2, "tooted" ×2).
- **Solution:**
    - Replace the untyped block with `Organization` (plus `Product` on product pages) so it is eligible for rich results.
    - Disambiguate repeated anchors with `aria-label` or surrounding context, e.g. `<a href="/kontakt/" aria-label="Kontakt – võta ESTPLY-ga ühendust">kontakt</a>`.

3D. Complete the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only sets `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`. Site signals show no auth, payments, user content or e-commerce, so this is a low-risk hardening item rather than an urgent one.
- **Solution:** Start with a report-only policy, then enforce:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
base-uri 'self';
  frame-ancestors 'self'; script-src 'self' 'nonce-{random}'
'strict-dynamic';
  report-uri /csp-report
```

  Use nonces + `'strict-dynamic'` rather than a flat host allowlist.

3E. Add Referrer-Policy, Permissions-Policy, COOP/CORP and HSTS preload `Security`

- **Impact:** Privacy, origin isolation, HSTS coverage
- **Problem:** Security basics fails Referrer-Policy, Permissions-Policy, COOP, CORP and HSTS preload; HSTS is set to `max-age=31536000; includeSubDomains` without `preload`.
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=
(), camera=()"
```

```
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
```

Only submit to hstspreload.org once every subdomain is HTTPS-ready.

3F. Add Subresource Integrity to the jsDelivr script `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** Security basics warns that 1 of 1 cross-origin scripts lacks an `integrity` attribute — `cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist/iframemanager.js`.
- **Solution:**

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist
/iframemanager.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

Generate the hash from the exact pinned version and update it whenever the version changes.

3G. Fix srcset entries missing width descriptors `Best Practices`

- **Impact:** W3C validity, responsive image selection
- **Problem:** W3C reports 2 errors: `srcset` on the two `img.image__img` elements has no width specified while `sizes` is present.
- **Solution:**

```
<img src="…6c041c12….png"
     srcset="…6c041c12-251w.png 251w, …6c041c12-502w.png 502w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="" loading="lazy">
```

3H. Make the HTML document cacheable `Performance`

- **Impact:** Repeat-visit TTFB, cache hit ratio
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` equal to the request time, so browsers revalidate on every navigation despite WP Rocket being active.
- **Solution:**
  - Let WP Rocket manage the document cache and emit a positive `max-age` (e.g. `max-age=600, must-revalidate`) for anonymous visitors.

- Keep `Vary: Accept-Encoding` (already present).
- Ensure logged-in / dynamic regions bypass the cache.

3I. Verify contrast on the 7 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast
- **Problem:** axe-core returned 0 violations but flagged 7 nodes as "incomplete" for color-contrast, so contrast on those elements is unverified.
- **Solution:**
  - Inspect the 7 nodes manually in DevTools (contrast ratio ≥4.5:1 for body text, ≥3:1 for large text).
  - Pay attention to text over gradients or semi-transparent backgrounds, which axe skips.

3J. Emit valid structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The `structuredData` SEO audit fails and the single JSON-LD block is typed "Unknown", so no recognized schema is exposed.
- **Solution:**
  - Add an `Organization` (or `WebPage` for this legal page) JSON-LD block with `@context`, `@type`, `name`, `url`.
  - Validate with Google's Rich Results Test and the Schema Markup Validator.

3K. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self'` — missing `default-src` and `object-src 'none'`, so no script or resource restrictions apply.
- **Solution:** The site has no auth, payments, UGC or commerce, so this is low-risk — but the header is already present, so completing it is cheap:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
base-uri 'self'; frame-ancestors 'self'; script-src 'nonce-
{random}' 'strict-dynamic' https:; style-src 'self' 'unsafe-inline'
```

  - Use the nonce/ `'strict-dynamic'` pattern rather than a flat allowlist.

3L. Resolve the WP Rocket script-type validation errors `Best Practices`

- **Impact:** W3C validity (6 of 8 errors)
- **Problem:** W3C reports 5 errors for `defer` and 1 for `async` on `<script type="text/rocketlazyloadscript">` data blocks, plus 2 warnings for redundant

`type="text/javascript"`.

- **Solution:**
  - These come from WP Rocket's lazyload rewrite; the practical impact is low, but the markup is invalid.
  - Either let WP Rocket rewrite to a real `type="module"` /JS MIME type, or move the deferred loading to a `<link rel="preload">` + small loader.
  - Remove `type="text/javascript"` from classic scripts (it is the default).

3M. Disambiguate vague link text and fix the JSON-LD type `SEO`

- **Impact:** Anchor-text relevance; rich-result eligibility
- **Problem:** 38 anchors include repeated vague text ("siin" ×2, "meist" ×2, "tooted" ×2, "kontakt" ×2) and the single JSON-LD block has type "Unknown", which Lighthouse flags via `structuredData`.
- **Solution:**
  - Replace "siin" with descriptive text, e.g. "lugege meie privaatsuspoliitikat".
  - Use a recognised schema type (`WebPage` / `PrivacyPolicy` via `WebPage` + `about`) instead of the unrecognized block.
  - Add `aria-label` where surrounding context cannot disambiguate.

3N. Add Referrer-Policy, Permissions-Policy, COOP and CORP `Security`

- **Impact:** Privacy leakage, cross-origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing from the response headers.
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

3O. Add HSTS preload and SRI on the jsDelivr script `Security`

- **Impact:** Transport hardening, third-party script integrity
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` without `preload`, and the single cross-origin script (`cdn.jsdelivr.net/.../iframemanager.js`) has no `integrity` attribute.
- **Solution:**
  - Append `; preload` to the HSTS header and submit the domain at hstspreload.org.

- Pin the CDN script:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist
/iframemanager.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

3P. Block /wp-admin/install.php and trim the Server header `Security`

- **Impact:** Attack surface, technology disclosure
- **Problem:** The security scan found `/wp-admin/install.php` reachable and the response discloses `Server: Apache / ZoneOS`.
- **Solution:**

```
<Files "install.php">
  Require all denied
</Files>
ServerTokens Prod
ServerSignature Off
```

3Q. Set a real Cache-Control for the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, cache efficiency
- **Problem:** The document response sends `cache-control: max-age=0` despite WP Rocket being active, forcing revalidation on every navigation.
- **Solution:**
  - Keep HTML short-lived but cacheable, e.g. `Cache-Control: public, max-age=600, s-maxage=3600, stale-while-revalidate=86400`.
  - Ensure WP Rocket's page cache is warmed for `/kupsiste-poliitika/` so the first visitor does not pay the cold-start cost.

3R. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor-text relevance, screen-reader link lists
- **Problem:** The inventory lists repeated generic anchors — "meist" ×2, "tooted" ×2, "ressursid" ×2, "kontakt" ×2, "liitu meiega" ×2 — which are ambiguous out of context.
- **Solution:**
  - Make anchor text self-describing (e.g. "Kontakt – estply OÜ" instead of "kontakt").
  - Or add `aria-label` to disambiguate icon/duplicate links:

```
<a href="/kontakt/" aria-label="Võta estplyga ühendust">kontakt</a>
```